UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

KATHRYN COSTA, NATALENE GAUNA, GREG LEEB, KAREN STIVALETTA, KERRI SHAPIRO, and LORI TRENT, Individually and on Behalf of a Class of All Others Similarly Situated, Plaintiffs, v. MARRIOTT INTERNATIONAL, INC., and STARWOOD HOTELS & RESORTS WORLDWIDE LLC, Defendants.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED January 31, 2019

Plaintiffs Kathryn Costa, Natalene Gauna, Greg Leeb, Karen Stivaletta, Kerri Shapiro, and Lori Trent (collectively, "Plaintiffs"), by and through their undersigned counsel, upon personal knowledge, as to themselves and their own acts, and upon information and belief, as to all other matters, bring this putative class action against Defendants Marriott International, Inc. ("Marriott") and Starwood Hotels & Resorts Worldwide LLC ("Starwood") (collectively, "Defendants") and allege as follows:

INTRODUCTION

1. Plaintiffs individually and on behalf of all others similarly situated bring this class action on behalf of persons who have suffered, and continue to suffer, financial losses and increased data security risks that are a direct result of Defendants' egregious failure to safeguard their customers' highly sensitive personally identifiable information ("PII"), including, but not limited to, names, mailing addresses, phone numbers, email addresses, passport numbers, preferred guest account information, date of birth, gender, arrival and departure information,

reservation dates, communication preferences, and payment card data, including, but not limited to, credit and debit card numbers, primary account numbers, card verification value numbers, expiration dates, and zip codes (the "Payment Card Data").[1] The breach impacted Defendant Starwood's guest database and affected persons who made reservations at any of Marriott's Starwood properties.

2. Specifically, between at least 2014 and September 2018, Defendants were subject to one of the longest-running and largest data breaches in history. During this time period, intruders gained and maintained unabated access to the PII and Payment Card Data of approximately 500 million guests who made a reservation at one of Marriott's Starwood properties. Despite the fact that the threat of a data breach has been a well-known risk to Defendants, Defendants failed to take reasonable steps to adequately protect the ultra-sensitive, highly sought after PII and Payment Card Data of hundreds of millions of individuals. Plaintiffs and the Class are now left to deal with the direct consequences of Defendants' failures.

3. The data breach was the inevitable result of Defendants' lax approach to the security of consumers' PII and Payment Card Data, an approach characterized by neglect, incompetence, and an overarching desire to minimize costs.[2]

4. Defendants' data security deficiencies were so significant that, even after hackers entered their systems, their activities went undetected for at least four years, despite obvious red

[1] Marriott has announced that stolen Payment Card Data was protected by encryption technology, but could not rule out the possibility the hackers had also accessed the encryption keys needed to decrypt the data. *See* Press Release, Marriott Int'l, Inc., Marriott Announces Starwood Guest Reservation Database Security Incident (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.

[2] Marriott President and Chief Executive Officer, Arne Sorenson, acknowledged that Marriott '"fell short of what our guests deserve and what we expect of ourselves"' in the November 30, 2018 release announcing the breach. *Id.*

flags that should have caused Defendants to discover their presence and thwart – or at least minimize – the damage.

5. For example, on November 20, 2015, just days after the announcement of its acquisition by Marriott, Starwood disclosed a security breach involving the compromise of the Payment Card Data for customers of more than 50 of its hotel properties. According to Starwood's disclosure, this breach had carried on undiscovered for as long as one year. Starwood later restated that the number of affected hotels exceeded 100.[3]

6. Defendants' actions have left Starwood customers' PII and Payment Card Data exposed and accessible to hackers for years. Consequently, Plaintiffs and the Class have incurred, and will continue to incur, significant damages in taking protective measures to reduce risk of identity theft and other fraudulent activity, as well as misuse of Payment Card Data, among other things.

7. Plaintiffs seek to recover the costs that they and others similarly situated have been forced to bear as a direct result of Defendants' data breach and to obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the unprecedented scope of this breach.

PARTIES

8. Plaintiff Kathryn Costa ("Costa") is a citizen of the State of South Carolina. During the Class Period, Plaintiff Costa provided Defendants her PII and Payment Card Data for the rental of Starwood hotel rooms. As a result of Defendants' actions, Plaintiff Costa has been

[3] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WALL. ST. J. (Dec. 2, 2018, 5:11 p.m. ET), https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

injured, has financial losses, and will be subject to a substantial risk for further identity theft due to Defendants' data breach.

9. Plaintiff Natalene Gauna ("Gauna") is a citizen of the State of Michigan. During the Class Period, Plaintiff Gauna provided Defendants her PII and Payment Card Data for the rental of Starwood hotel rooms. As a result of Defendants' actions, Plaintiff Gauna has been injured, has financial losses, and will be subject to a substantial risk for further identity theft due to Defendants' data breach.

10. Plaintiff Greg Leeb ("Leeb") is a citizen of the State of Georgia. During the Class Period, Plaintiff Leeb provided Defendants his PII and Payment Card Data for the rental of Starwood hotel rooms. As a result of Defendants' actions, Plaintiff Leeb has been injured, has financial losses, and will be subject to a substantial risk for further identity theft due to Defendants' data breach.

11. Plaintiff Karen Stivaletta ("Stivaletta") is a citizen of the State of New Hampshire. During the Class Period, Plaintiff Stivaletta provided Defendants her PII and Payment Card Data for the rental of Starwood hotel rooms. As a result of Defendants' actions, Plaintiff Stivaletta has been injured, has financial losses, and will be subject to a substantial risk for further identity theft due to Defendants' data breach.

12. Plaintiff Kerri Shapiro ("Shapiro") is a citizen of the State of New York. During the Class Period, Plaintiff Shapiro provided Defendants her PII and Payment Card Data for the rental of Starwood hotel rooms. As a result of Defendants' actions, Plaintiff Shapiro has been injured, has financial losses, and will be subject to a substantial risk for further identity theft due to Defendants' data breach.

13. Plaintiff Lori Trent ("Trent") is a citizen of the State of West Virginia. During the Class Period, Plaintiff Trent provided Defendants her PII and Payment Card Data for the rental of Starwood hotel rooms. As a result of Defendants' actions, Plaintiff Trent has been injured, has financial losses, and will be subject to a substantial risk for further identity theft due to Defendants' data breach.

14. Defendant Marriott is a publicly traded corporation with its principal place of business at 10400 Fernwood Road, Bethesda, Maryland 20817.

15. Defendant Starwood is an indirect, wholly owned subsidiary of Marriott. On September 23, 2016, Marriott completed the acquisition of Starwood Hotels & Resorts Worldwide, LLC, formerly known as Starwood Hotels & Resorts Worldwide, Inc.

JURISDICTION AND VENUE

16. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 putative Class (defined below) members; and minimal diversity exists because the majority of putative Class members, including the named Plaintiffs, are citizens of a different state than Defendants.

17. This Court has personal jurisdiction over Defendant Starwood as it maintains its principal headquarters in Connecticut, is registered to conduct business in Connecticut, regularly conducts business in Connecticut, and has sufficient minimum contacts in Connecticut. Defendants intentionally avail themselves of this jurisdiction by conducting Starwood's corporate operations here and promoting, selling, and marketing Starwood's services to resident Connecticut consumers and entities.

18. Venue is proper in this District under 28 U.S.C. §1391(a) because Starwood's principal place of business is in Connecticut and a substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiffs occurred in this District.

FACTUAL ALLEGATIONS

A. Background

19. Founded in 1927, Marriott is the largest hotel chain in the world. Owning more than 6,500 properties in 127 countries and territories, Marriott had $22.894 billion in revenue in 2017. Its common stock is traded on the NASDAQ under the ticker symbol "MAR."

20. Starwood is a subsidiary of Marriott. The acquisition of Starwood by Marriott was announced on November 16, 2015 and finalized on September 23, 2016.

21. Starwood collected PII and Payment Card Data directly from consumers who made a reservation using Starwood's guest reservation database at a Starwood property. During the Class Period, Defendants collected and maintained a substantial and diverse amount of PII and Payment Card Data.

B. Plaintiffs and the Class Relied on Marriott to Adequately Protect Their Sensitive Information

22. Defendants have a well-established and clear legal duty to act reasonably to protect PII and Payment Card Data they collect and possess from exposure to unauthorized third parties.

23. When Plaintiffs and the Class provided Defendants with their most sensitive information, or when Defendants received such information in some other manner, Plaintiffs and the Class reasonably expected that such information would be stored by Defendants in a safe and confidential manner, using all reasonable safeguards and protections.

C. **The Marriott Data Breach**

24. On November 30, 2018, Defendants announced a data security incident involving the Starwood guest reservation database.

25. According to a November 30, 2018 announcement by Marriott:

> Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. ***Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014.***[4]

26. Marriott's announcement further identified the massive scope of the breach and the range of PII and Payment Card Data compromised over the preceding four-year period.

> The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately ***500 million guests*** who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of ***name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates***, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information.[5]

27. Marriott reportedly discovered this breach on September 8, 2018, yet took months to publicly disclose the existence to the public:

> On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had

[4] Marriott Announces Starwood Guest Reservation Database Security Incident, *supra* n.1 (emphasis added).

[5] *Id.* (emphasis added).

> been unauthorized access to the Starwood network since 2014. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.[6]

D. The Breach Was the Result of Defendants' Failure to Properly and Adequately Secure Their U.S. Website

28. The data security breach was the direct result of Defendants' actions and choices, which resulted in inadequate data security of the systems containing PII and Payment Card Data.

29. Among other things, the November 20, 2015 announcement of the Starwood data breach, which occurred within four days of the companies' announcement of the merger, should have alerted Defendants to obvious security deficiencies. Defendants should have recognized and identified the flaws in Starwood guest reservation systems and its data security and should have taken measures to fix these vulnerabilities.[7]

30. The harm to Plaintiffs resulting from Defendants' improper actions that led to Defendants' inadequate and insufficient security of their computer systems and websites was at all times entirely foreseeable to Defendants.

31. Defendants are well aware of the costs and risks associated with payment card fraud and identity theft, as acknowledged in their regulatory filings:

> Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. The integrity and protection of that customer, employee, and company data is critical to our business.
>
> * * *

[6] *Id*.

[7] Robert McMillan, *supra* n.3.

> Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information.[8]

E. Defendants Knew that a Breach of Their Computer Systems Was a Foreseeable Risk

32. With data breaches and identity theft on the rise, Defendants undoubtedly knew that a breach of their computer systems was a foreseeable risk. They also knew what the repercussions of such a breach would be.

33. PII and Payment Card Data have considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell such stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[9]

34. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. According to the Identity Theft Resource Center ("ITRC"), in 2018, there were 1,244 reported data breaches in the United States and more than 446.52 million records reportedly were exposed in those breaches.[10]

35. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2017, affecting approximately 16.7 million victims in the United States, with the amount stolen rising to $16.8 billion.[11]

---

[8] Marriott Int'l, Inc., Quarterly Report at 55 (Form 10-Q) (Nov. 9, 2016).

[9] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[10] *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RES. CTR. (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-1.pdf.

[11] Press Release, Javelin Strategy & Research, Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

36. Following several high-profile data breaches in recent years, including those involving Target, Experian, Yahoo, Home Depot, and Sony, Defendants were on notice of the very real risk that hackers could exploit vulnerabilities in Defendants' data security.

37. Thus, Defendants knew, given the vast amount of PII they managed, that they were a target of attempted cyber and other security threats and therefore understood the risks posed by their insecure and vulnerable computer systems and website. They also understood the need to safeguard PII and the impact a data breach would have on their customers, including Plaintiffs and the Class.

F. Defendants Violated Federal Security Requirements and Other Industry Standards

38. Defendants have a clear legal duty to maintain the confidentiality of consumers' sensitive information and prevent any third-party misuse or access to such information. Defendants' actions and failure to safeguard customer information violated federal data security standards and industry standards, as well as a clearly established legal duty to not act negligently when handling and storing PII and Payment Card Data.

G. Defendants Failed to Comply with Federal Trade Commission Requirements

39. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914 (the "FTC Act"), 15 U.S.C. §45.

40. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's

vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC also has published a document, entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

42. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

43. In the months and years leading up to the data breach, and during the course of the breach itself, Defendants failed to follow the guidelines recommended by the FTC. Further, by failing to have reasonable data security measures in place, Defendants engaged in unfair acts or practices within the meaning of §5 of the FTC Act.

H. Defendants Failed to Comply with Industry Standards for Data Security

44. The Payment Card Industry Security Standards Council promulgates a set of minimum requirements, which apply to all organizations that store, process, or transmit Payment Card Data. This standard, known as the Payment Card Industry Data Security Standard ("PCI DSS"), is the industry standard governing the security of Payment Card Data. It sets the minimum level of what must be done, not the maximum.

45. PCI DSS v.3.2, the version of the standard in effect beginning in April 2016, imposes the following 12 "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Furthermore, PCI DSS v.3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

46. Among other things, PCI DSS required Marriott to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; implement proper network segmentation; encrypt Payment Card Data at the point-of-sale; restrict access to Payment Card Data to those with a need to know; and establish a process to identify and timely fix security vulnerabilities. As discussed herein, Marriott failed to comply with each of these requirements.

I. Plaintiffs and the Class Have Been, Are Currently Being, and Will Be Harmed by the Data Breach

47. The data breach has inflicted immediate, hard costs on Plaintiffs and members of the Class.

48. Defendants failed to follow industry standards and failed to effectively monitor their security systems to ensure the safety of customer information. Defendants' substandard security protocols and failure to adequately monitor for unauthorized intrusion caused Plaintiffs and the Class's PII and Payment Card Data to be compromised for years without detection by Defendants.

49. Plaintiffs and the Class have incurred, and will continue to incur, substantial damage because of Defendants' failures to meet reasonable standards of data security.

50. As a result of the Defendants' data breach, Plaintiffs and the Class are required to cancel payment cards, change or close accounts, investigate fraudulent activity, and take other steps to protect themselves in an effort to reduce the risk of future, but certainly impending, identity theft, loan fraud, and other fraudulent transactions.

51. Sensitive personal and financial information, like the information compromised in this breach, is extremely valuable. Criminals have gained access to complete profiles of individuals' personal and financial information. They can now use this data to steal the identities of the consumers whose information has been compromised or sell it to others who plan to do so. In this manner, unauthorized third parties can assume the stolen identities (or create entirely new identities from scratch) to make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the member's or customer's name, obtain government benefits, or file a fraudulent tax return. A report by the Department of Justice ("DOJ") found that 86% of identity theft victims in 2014 experienced the fraudulent use of existing account information, including credit card and bank account information.[12]

52. Consumers inevitably face significant emotional distress after theft of their identity. The fear of financial harm can cause significant stress and anxiety for many consumers. According to the DOJ, an estimated 36% of identity theft victims experienced moderate or severe emotional distress as a result of the crime.[13]

---

[12] Erika Harrell, Ph.D., *Victims of Identity Theft, 2014*, U.S. DEP'T OF JUST., BUREAU OF JUST. STAT. (Sept. 2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

[13] *Id.*

53. Ultimately, Plaintiffs and the Class are faced with considerable present injury, and an immediate future of continually unfolding new and continued injuries, as a result of Defendants' avoidable data breach.

CLASS ACTION ALLEGATIONS

54. Plaintiffs bring this action on behalf of themselves and as a class action under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following nationwide class or, in the alternative, six state subclasses:[14]

> **Nationwide Class:** All individuals legally residing in the United States who provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.
>
> **Georgia Subclass:** All individuals legally residing in Georgia who, while residing in Georgia, provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.
>
> **Michigan Subclass:** All individuals legally residing in Michigan who, while residing in Michigan, provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.
>
> **New Hampshire Subclass:** All individuals legally residing in New Hampshire who, while residing in New Hampshire, provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.
>
> **New York Subclass:** All individuals legally residing in New York who, while residing in New York, provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries

[14] The six state subclasses are collectively referred to herein as the "State Subclasses" and further, with the Nationwide Class, the "Class."

and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.

South Carolina Subclass: All individuals legally residing in South Carolina who, while residing in South Carolina, provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.

West Virginia Subclass: All individuals legally residing in West Virginia who, while residing in West Virginia, provided PII or payment card information for the Starwood guest reservation system to Defendants or any of their affiliates or subsidiaries and whose information was accessed, copied, or stolen by an unauthorized party in the data breach event initially announced on November 30, 2018.

The Rule 23(a) Factors

55. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

56. **Numerosity.** The members of the Class are so numerous that joinder would be impracticable. Plaintiffs believe the number of Class members exceeds 1,000,000.

57. **Commonality.** There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

a. whether Defendants owed a duty to Plaintiffs and members of the Class to protect PII and Payment Card Data;

b. whether Defendants failed to provide reasonable security to protect PII and Payment Card Data;

c. whether Defendants negligently or otherwise improperly allowed PII and Payment Card Data to be accessed by third parties;

d. whether Defendants failed to adequately notify Plaintiffs and members of the Class that their data systems were breached;

e. whether Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses;

f. whether Defendants' actions, which failed to reasonably secure Plaintiffs' and the Class's PII and Payment Card Data, proximately caused the injuries suffered by Plaintiffs and members of the Class;

g. whether Plaintiffs and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. whether Plaintiffs and members of the Class are entitled to declaratory and injunctive relief.

58. **Typicality.** Plaintiffs' claims are typical of the claims of the absent Class members and have a common origin and basis. Plaintiffs and Class members are all persons and entities injured by Defendants' data breach. Plaintiffs' claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely, the Defendants' data breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief.

59. **Adequacy.** Plaintiffs will fully and adequately assert and protect the interests of the absent Class members and has retained Class counsel who have considerable experience in class action litigation concerning corporate data security and the resources necessary to prosecute this case. Neither Plaintiffs nor their attorneys have any interests contrary to or conflicting with the interests of absent class members.

The Rule 23(b)(3) Factors

60. The questions of law and fact common to all Class members predominate over any questions affecting only individual Class members.

61. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiffs know of no difficulties in managing this action that would preclude its maintenance as a class action.

62. Contact information for each Class member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

COUNT I
Negligence
(Brought by All Plaintiffs and the Nationwide Class)

63. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

64. Defendants owed Plaintiffs and the Class a common-law duty to exercise reasonable care in the collection and storage of their PII and Payment Card Data.

65. Defendants' duty included an obligation to take reasonable protective measures against the foreseeable risk to Plaintiffs and the Class that harm would inevitably result if their PII or Payment Card Data was interfered with, stolen, or copied while in Defendants' possession.

66. Defendants knew or should have known that by collecting and storing PII and Payment Card Data, they created a valuable trove of information that was a foreseeable target for third-party interference, copying, or theft.

67. Defendants knew, or should have known, that companies possessing similar data troves have in fact been targeted for hacking in highly publicized data breaches, including Yahoo, Equifax, Wyndham, Home Depot, and Sony, to name just a few.

68. Once Defendants chose to collect and store PII and Payment Card Data belonging to Plaintiffs and the Class, only Defendants were in a position to secure their valuable data trove from the foreseeable risk of third-party interference, copying, or theft.

69. Defendants' duty to act reasonably in collecting and storing PII and Payment Card Data also arises under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII and Payment Card Data.

70. Plaintiffs and the Class reasonably assumed that major corporations like Defendants would adhere to basic industry standards with respect to the collection and storage of PII and Payment Card Data; for instance – but not limited to – the PCI-DSS standards.

71. Defendants breached their common law and statutory duties by failing to use reasonable data collection, storage, and security practices. In addition to Defendants' initial negligence in storing PII and Payment Card Data on a system vulnerable to outside penetration, Defendants' negligence persisted for at least four years, during which Defendants failed to detect the ongoing compromise and failed to improve security practices in a way that could end the breach. During those years, Defendants missed numerous opportunities to stop or mitigate the data breach at a point in time when fewer individuals might have been harmed.

72. Defendants' negligent data collection and storage practices led to a foreseeable result: the valuable PII and Payment Card Data associated with Plaintiffs and the Class was copied or stolen by unauthorized third parties, who are now well-equipped to perpetrate fraud and identity theft at the expense of Plaintiffs and the Class.

73. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have been harmed in several ways. They are all now at an increased risk of being victims of identity theft, financial impersonation, and a variety of other fraudulent schemes, including those that use targeted phishing or social engineering techniques facilitated by the use of compromised PII elements against victims. To guard against the heightened risk of these crimes, Plaintiffs and the Class will need to invest more of their time and money on monitoring their finances, tax records, credit scores, and accounts of all types, including financial institutions, social media, loyalty programs, online retailers, and others.

74. Plaintiffs and the Class have suffered, and continue to suffer, injury, including, but not limited to, investing time and money in cancelling payment cards, changing or closing accounts, and taking other steps to monitor their identities and protect themselves.

75. But for Defendants' negligence, the PII and Payment Card Data of Plaintiffs and the Class would not have been exposed, or in the alternative, Plaintiffs and the Class would have at least learned of the compromise at an earlier point in time when some of their damages may have been mitigated.

COUNT II
Negligence *Per Se*
(Brought by All Plaintiffs and the Nationwide Class)

76. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

77. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII and Payment Card Data. The FTC publications and orders described above also form part of the basis of Defendants' duty.

78. Defendants violated §5 of the FTC Act by failing to use reasonable measures to protect PII and Payment Card Data and by not complying with applicable industry standards, including PCI-DSS, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and Payment Card Data they obtained and stored, length of time the information was maintained on an apparently vulnerable system, and foreseeable consequences of a data breach at a major, international hospitality company, including, specifically, the immense damages that would result to consumers.

79. Defendants' violations of §5 of the FTC Act constitute negligence *per se*.

80. Plaintiffs and members of the Class are consumers and are within the class of persons that §5 of the FTC Act was intended to protect.

81. The harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

82. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injury, including, but not limited to, investing time and money in cancelling payment cards, changing or closing accounts, and taking other steps to monitor their identities and protect themselves.

COUNT III
Declaratory and Equitable Relief
(Brought by Plaintiffs and the Nationwide Class)

83. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

84. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and violate the terms of the federal and state statutes described herein.

85. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure their customers' PII and Payment Card Data, specifically including information pertaining to PII and Payment Card Data used by Defendants' customers;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure their customers' PII and Payment Card Information; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiffs and the Class harm.

86. The Court also should issue corresponding injunctive relief requiring Defendants to employ adequate security protocols, consistent with industry standards, to protect PII and Payment Card Data. Specifically, this injunction should, among other things, direct Defendants to:

a. utilize industry standard encryption to encrypt the transmission of cardholder data at all times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. engage third-party auditors, consistent with industry standards, to test systems for weakness and upgrade any such weakness found;

e. audit, test, and train data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI-DSS standards pertaining to the security of customers' PII and Payment Card Data; and

h. install all upgrades recommended by manufacturers of security software and firewalls used by Defendants.

87. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach of Defendants' data occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

88. The hardship to Plaintiffs and the Class, if an injunction is not issued, exceeds the hardship to Defendants, if an injunction is issued. Among other things, if another massive data breach occurs with Defendants' data, Plaintiffs and members of the Class will likely incur tens of

millions of dollars in damages. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable data security measures is relatively minimal and Defendants have a pre-existing legal obligation to employ such measures.

89. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another breach of Defendants' systems, thus eliminating the injuries that would result to Plaintiffs, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court:

A. Certify the Nationwide Class and State Subclasses and appoint Plaintiffs and Plaintiffs' counsel to represent the Class;

B. Enter a monetary judgment in favor of Plaintiffs and the Class to compensate them for the injuries they have suffered, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

C. Enter a declaratory judgment as described herein;

D. Grant the injunctive relief requested herein;

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 31, 2019

SCOTT+SCOTT ATTORNEYS AT LAW LLP

/s/ Joseph P. Guglielmo

Joseph P. Guglielmo (CT 27481)
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com

Erin Green Comite (CT 24886)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Telephone: 860-537-5537
Facsimile: 860-537-4432
ecomite@scott-scott.com

Hal Cunningham
SCOTT+SCOTT ATTORNEYS AT LAW LLP
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: 619-233-4565
Facsimile: 619-233-0508
hcunningham@scott-scott.com

Gary F. Lynch
Jamisen A. Etzel
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com

Karen Hanson Riebel
Kate Baxter-Kauf
Arielle Wagner
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S, Suite 2200
Minneapolis, MN 55401
Telephone: 612-596-4097
Facsimile: 612-339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
aswagner@locklaw.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: 612-339-7300
Facsimile: 612-336-2921
bbleichner@chestnutcambronne.com

Counsel for Plaintiffs Kathryn Costa, Natalene Gauna, Greg Leeb, Karen Stivaletta, Kerri Shapiro, and Lori Trent